“DNS Flag day”

Removal of workarounds for EDNS

Hugo Salgado, .CL
Sebastián Castro, .NZ

GTER 46, São Paulo

nic chile
SOMOS EL PUNTO CL

InternetNZ

¿Do que se trata?

“Em 1º de fevereiro de 2019, os quatro principais provedores de software para DNS recursivo - Bind, Unbound, PowerDNS e Knot - lançarão conjuntamente novas versões de seus sistemas com uma característica comum: **o fim dos patches provisórios históricos** que eles perdoaram certos comportamentos que se desviaram do padrão em servidores DNS autoritativos."

De http://blog.nic.cl/2018/06/dns-flag-day-el-fin-de-los-parches.html (en español)

What is EDNS?

- RFC6891 (Apr. 2013, update from the original RFC2671 (1999))
  - Defines a backward compatible mechanism to signal support for new DNS options.
  - Original specification includes support for DNS responses larger than 512 bytes, extended response codes, etc.

How is it used?

- Maximum message size: from 512 bytes to 64 KB

- Current extensions:

- **NSID,** RFC 5001, nameserver identification string

- **DNSSEC**, DO bit, signal supports or interest for DNSSEC-related records

- **Client-subnet**, RFC 7871, signals the network the query comes from

- **Keep-alive**, RFC 7828, variable timeouts for DNS over TCP

- **Cookies**, RFC 7873, lightweight security mechanism

So, what’s the problem?

- Authoritative DNS servers block responses, or don’t answer, or answer with the wrong packet.
  - In general, bad implementations of DNS not following the standards

- Poorly implemented firewalls on the way, poor firewall rules blocking valid traffic or unaware of the standards

- Resolvers have to send a query, wait for a timeout and retry using a different method: TCP or discard EDNS
  - Forces delays and thwarts innovation and deployment of new features

What’s DNS Flag day?

- DNS implementations decided to remove workarounds in a coordinated way
- BIND, Unbound, PowerDNS and Knot will release new versions with the workarounds removed
- Public DNS resolvers will start being standard compliant (Google, Quad 9, Cloudflare)
- Feel the pain

  If you run inadequate software, your domains will break

How many domains could be affected?

- Coordinated effort to measure impact in .CL, .CZ, .SE, .NU and .NZ
- Many thanks to Petr Špaček from CZ.NIC for the Compliance Scanner, the .CZ, .SE and .NU data and the feedback
- Comparison against existing measures from ISC around root servers and TLDs nameservers

Measurement methodology

- “DNS Compliance Testing” tool written by ISC https://gitlab.isc.org/isc-projects/DNS-Compliance-Testing
  - Only check for EDNS compliance at this stage

- “EDNS Compliance scanner for DNS zones” from CZ.NIC:
  - https://gitlab.labs.nic.cz/knot/edns-zone-scanner/tree/master
  - Uniquely test all addresses of a nameserver
  - Preprocess a TLD zone and generate the minimal set of nameserver tests
  - Test multiple times to discard transient errors

Dead domains for latam

- .CL: 3.810 (0.88%)
  - 8.163 unique NS (top: 294 domains)
  - 63 in Alexa Top 1M
- .CO: 28.350 (1.28%)
- .GT: 131 (0.75%)
- 190.in-addr.arpa: 4.281 (20.05%)
- .SV: 214 (2.54%)

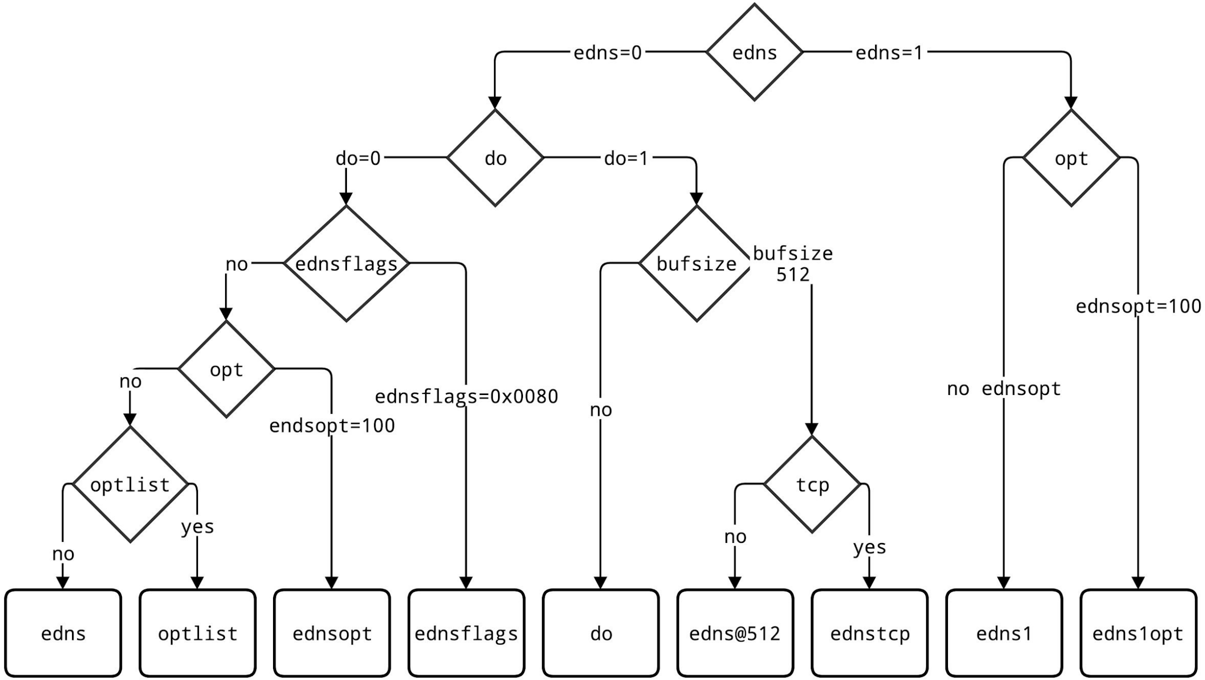
- **.com.br: 24.007 (0.72%)** (thanks Registro.BR!)

Test hierarchy

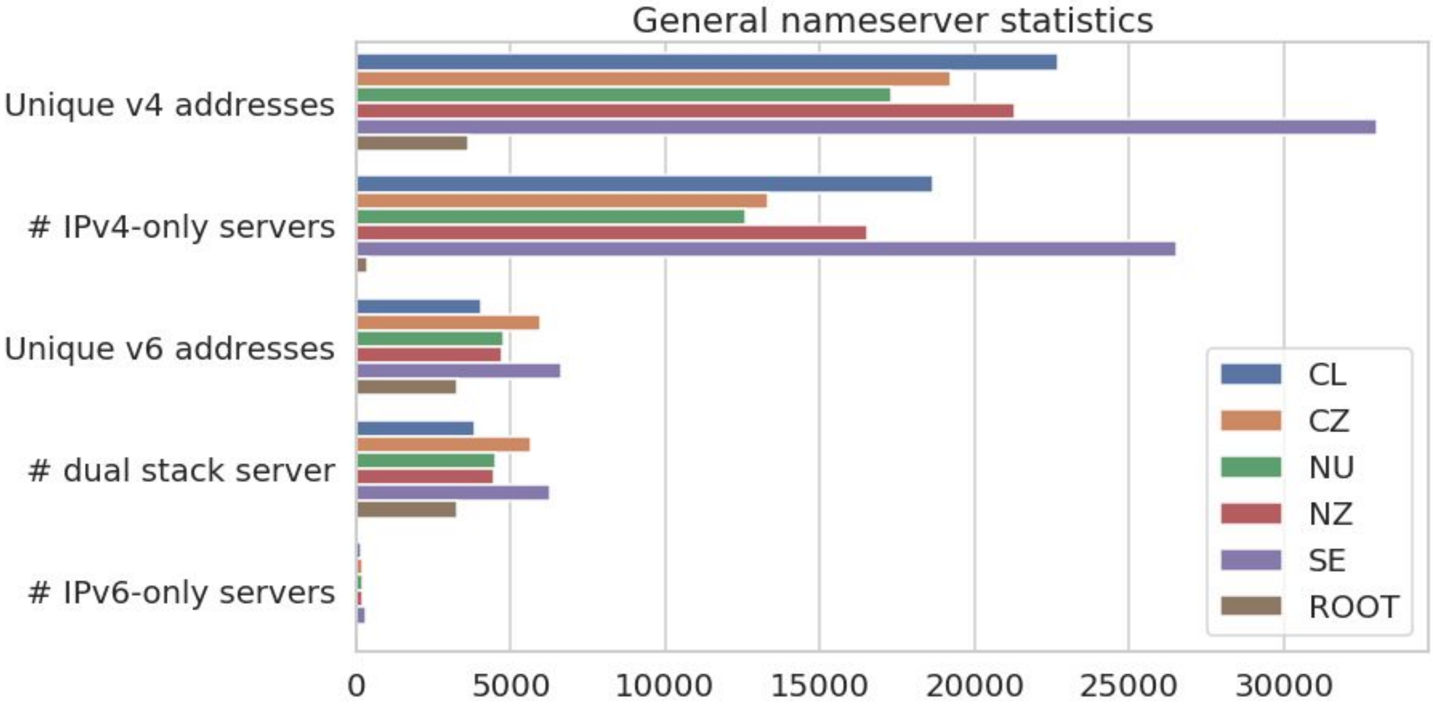
Different values and flags are added to the query

There are dependencies, increasing the complexity of the test

edns1opt requires edns1 and endsopt=100 to pass



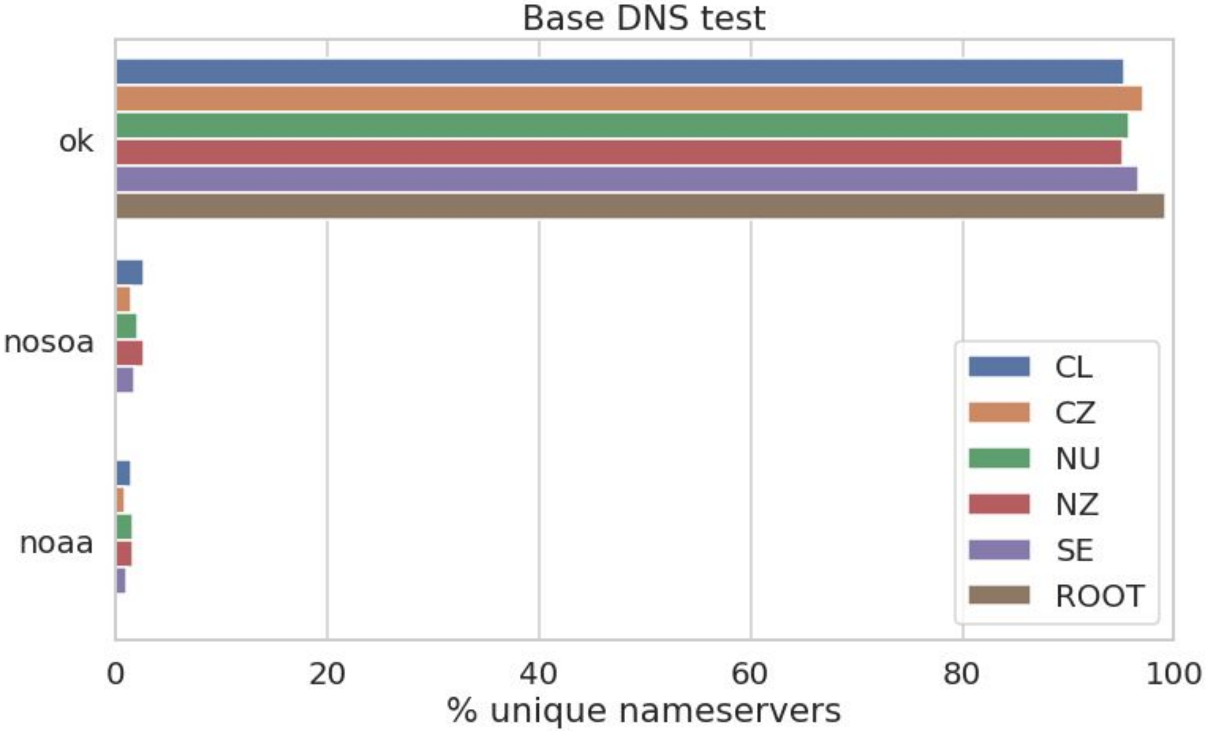
General statistics



DNS test results

dig +noedns +noad +norec SOA <ZONE>

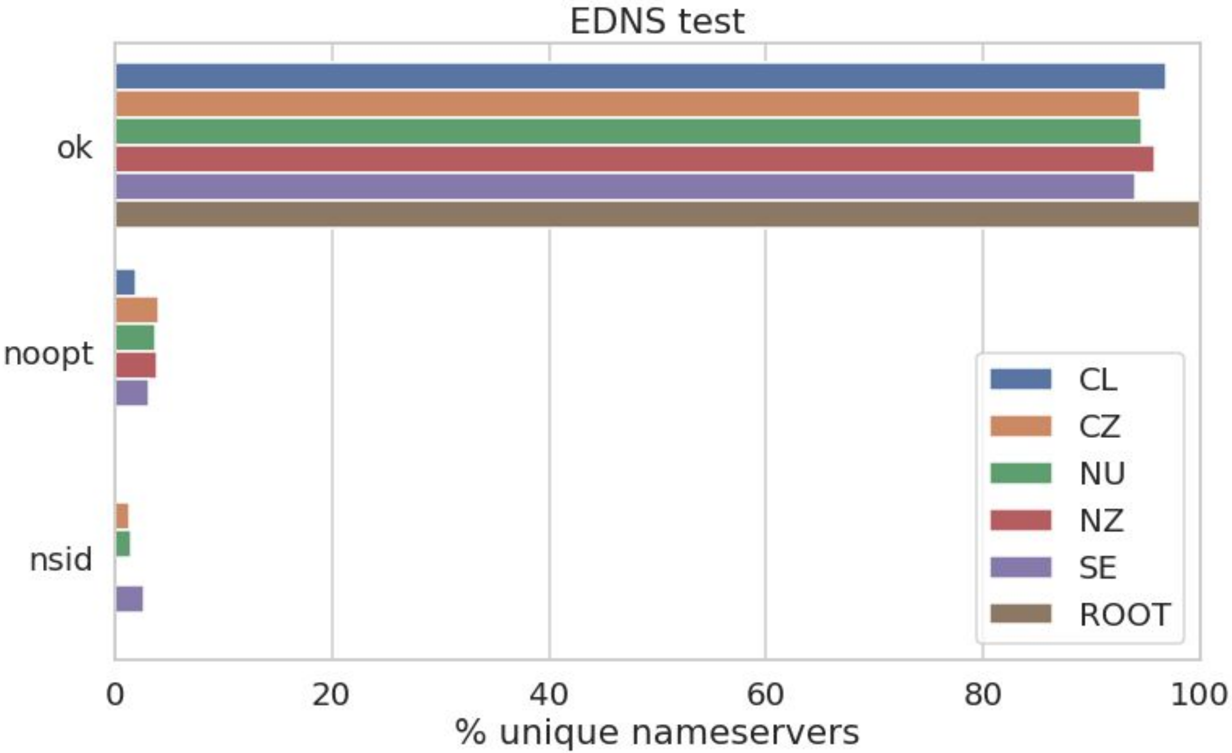
- ok: We got a good answer
- nosoa: Response didn’t have SOA record
- noaa: no AA bit in response



DNS vs EDNS

DNS: dig **+noedns** +noad +norec SOA <zone>

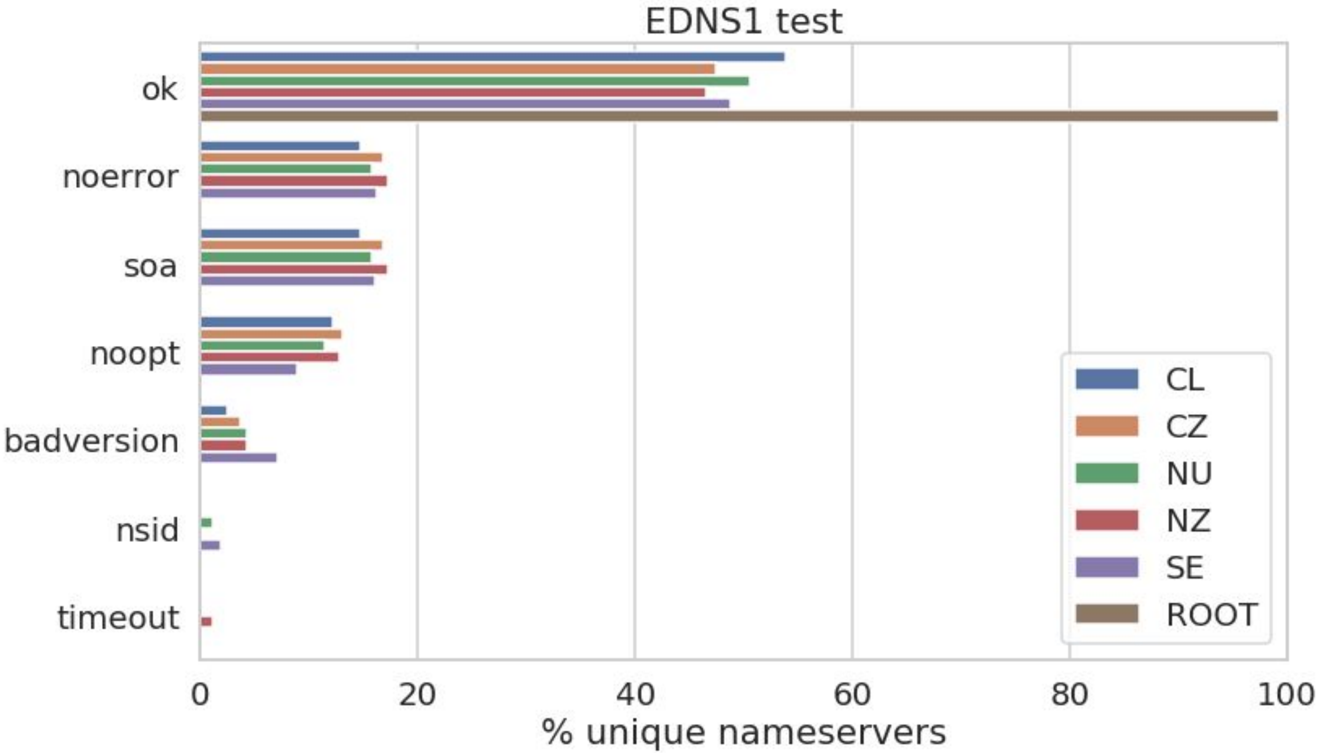
EDNS: dig **+edns=0 +nocookie** +noad +norec SOA <zone>



EDNS0 vs EDNS1

EDNS0: dig **+edns=0** +nocookie +noad +norec SOA <zone>

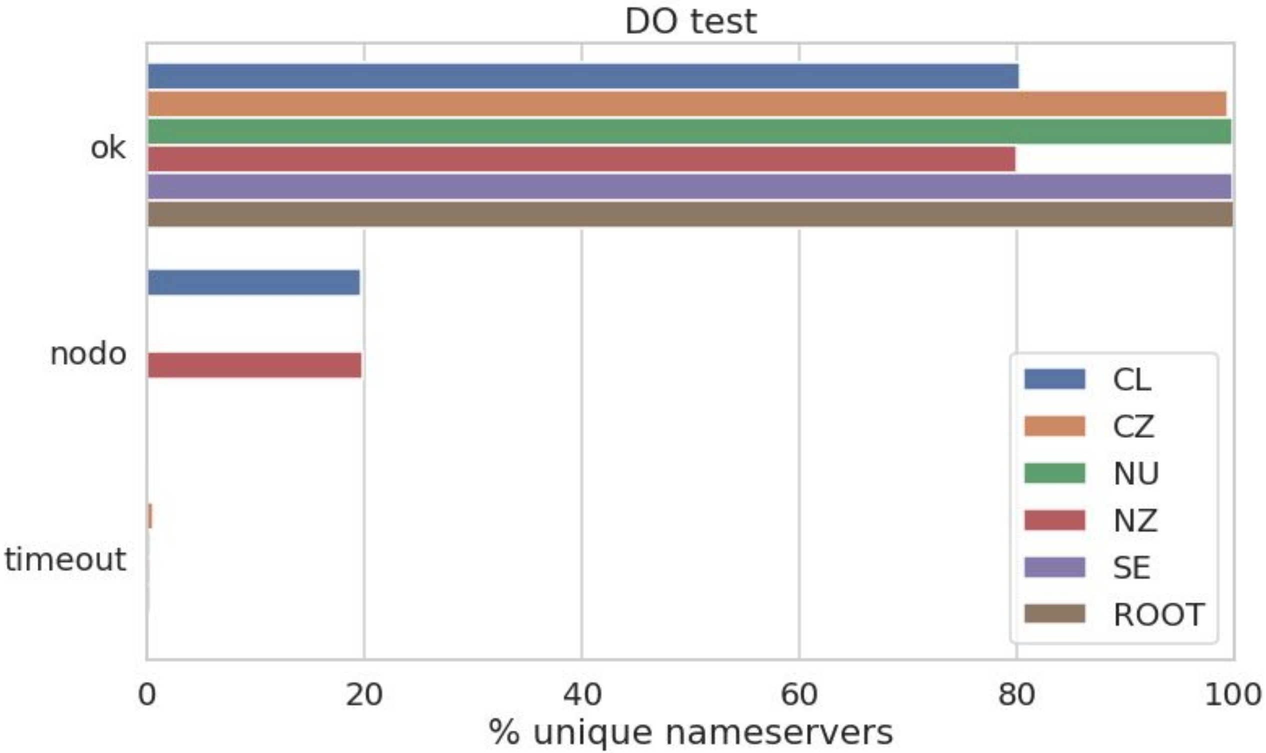
EDNS1: dig **+edns=1 +noednsneg** +nocookie +noad +norec SOA <zone>



EDNS vs DO

EDNS: dig +edns=0 +nocookie +noad +norec SOA <zone>

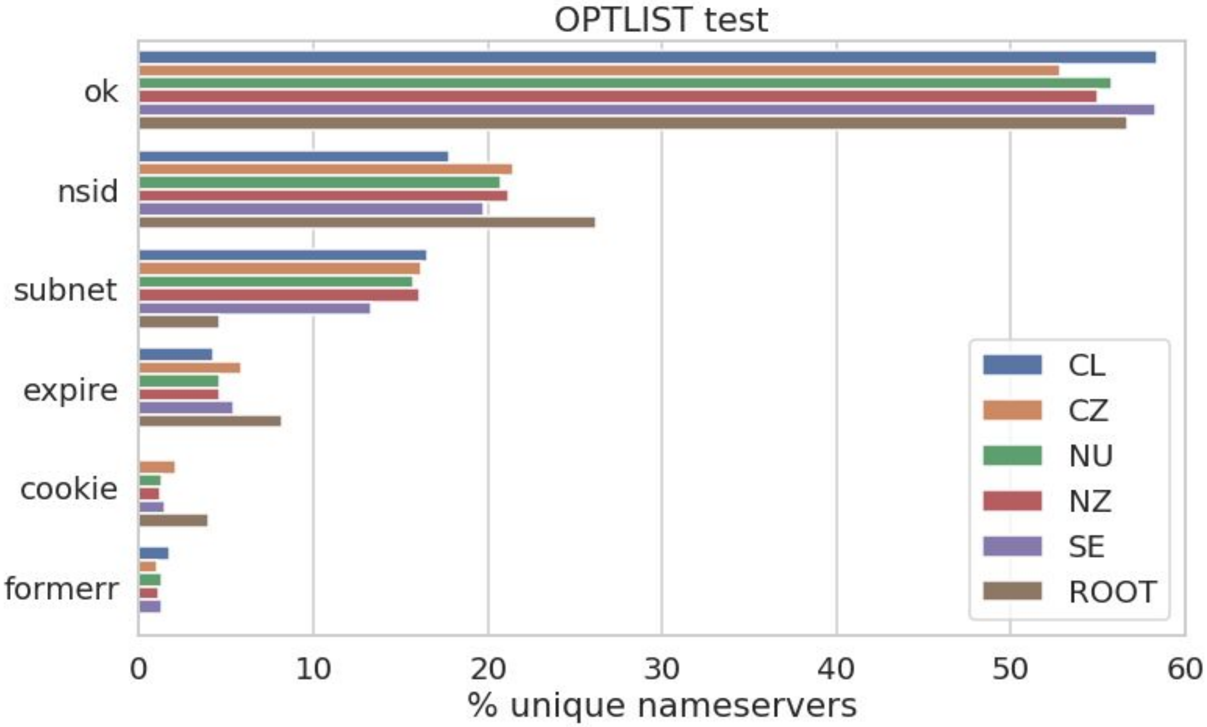
DO: dig +edns=0 +nocookie +noad +norec **+dnssec** SOA <zone>



EDNS vs OPTLIST

EDNS: dig +edns=0 +nocookie +noad +norec SOA <zone>

OPTLIST: dig +edns=0 +noad +norec **+nsid +subnet=0.0.0.0/0 +expire +cookie=0102030405060708** SOA <zone>



IPv4 vs IPv6

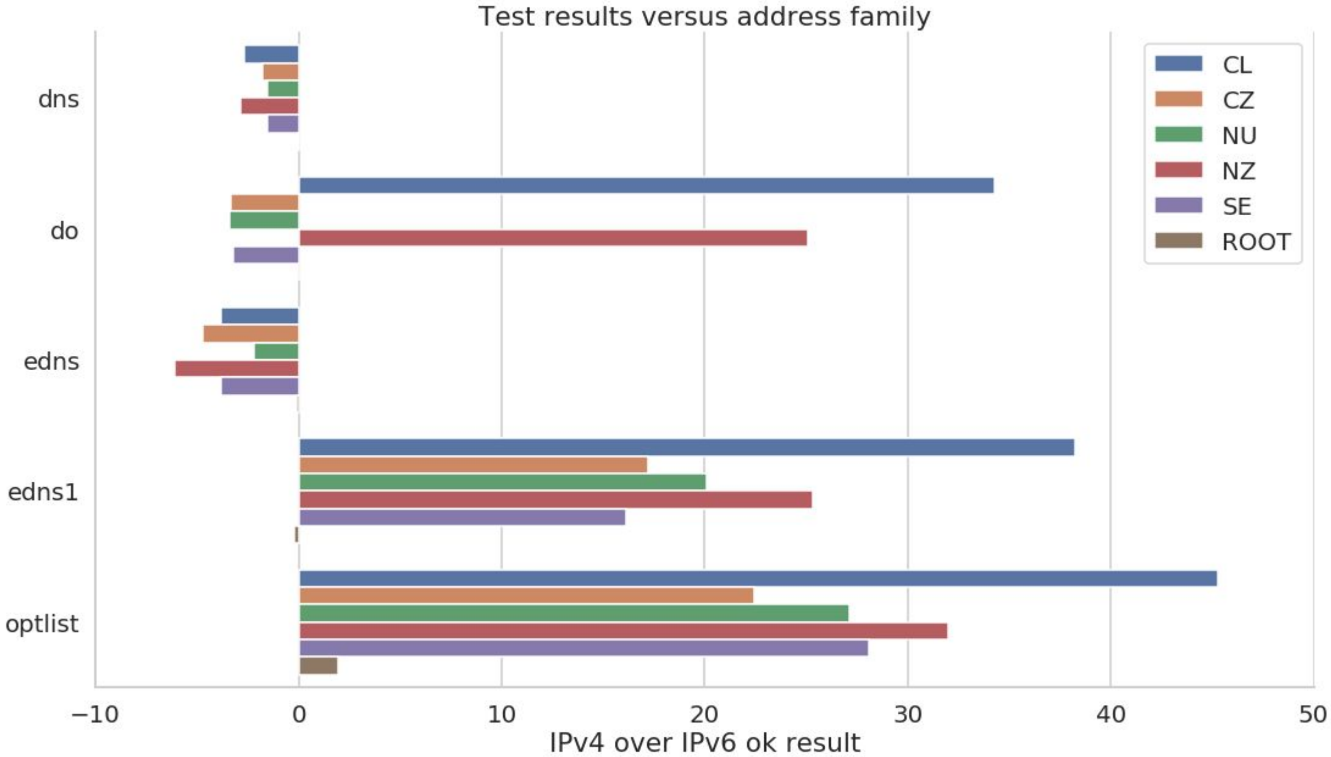
Is the behaviour of a given nameserver different depending on which address family was queried? Are they differences between IPv4 and IPv6

We can explore the tests that passed against the family of the address.

IPv4 vs IPv6

DNS and EDNS tests finish more successfully in IPv6 than IPv4!

EDNS1 and OPTLIST complete a lot more in IPv4 than IPv6!

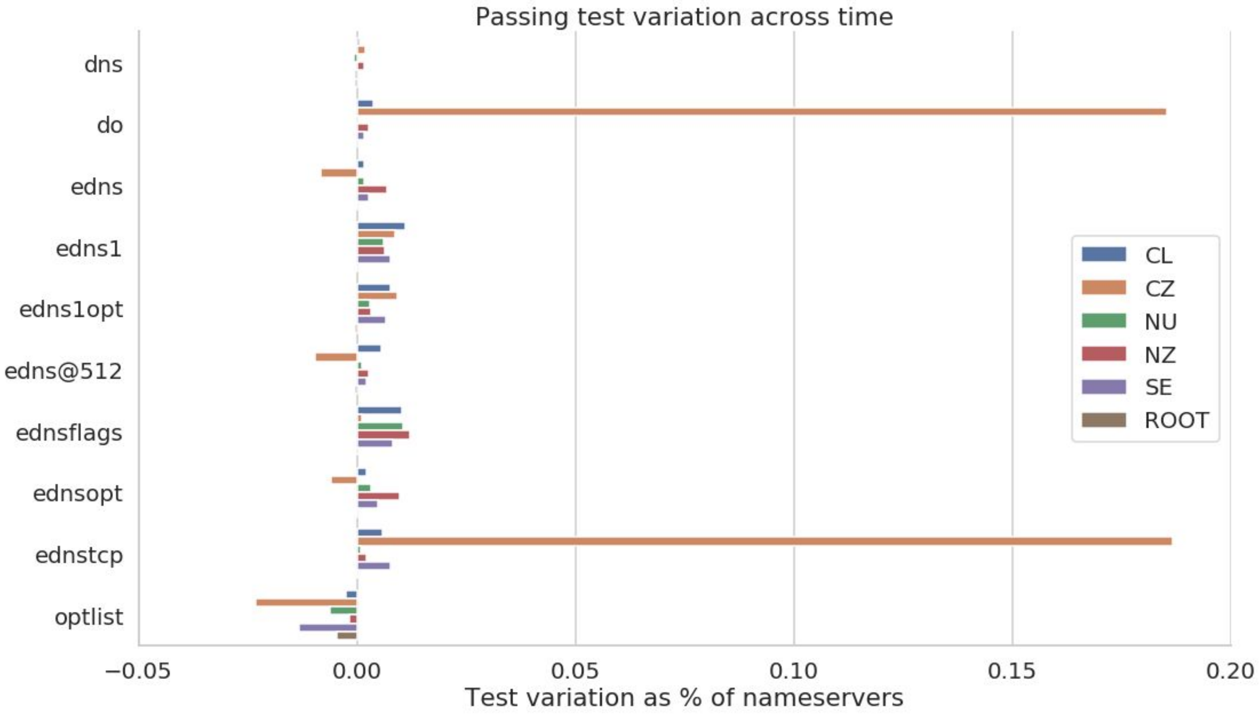


How the results change with time?

First data point is from May to July depending on the ccTLD

Last data point is from October.

CZ is seeing the improvements of their communication campaign.



In summary

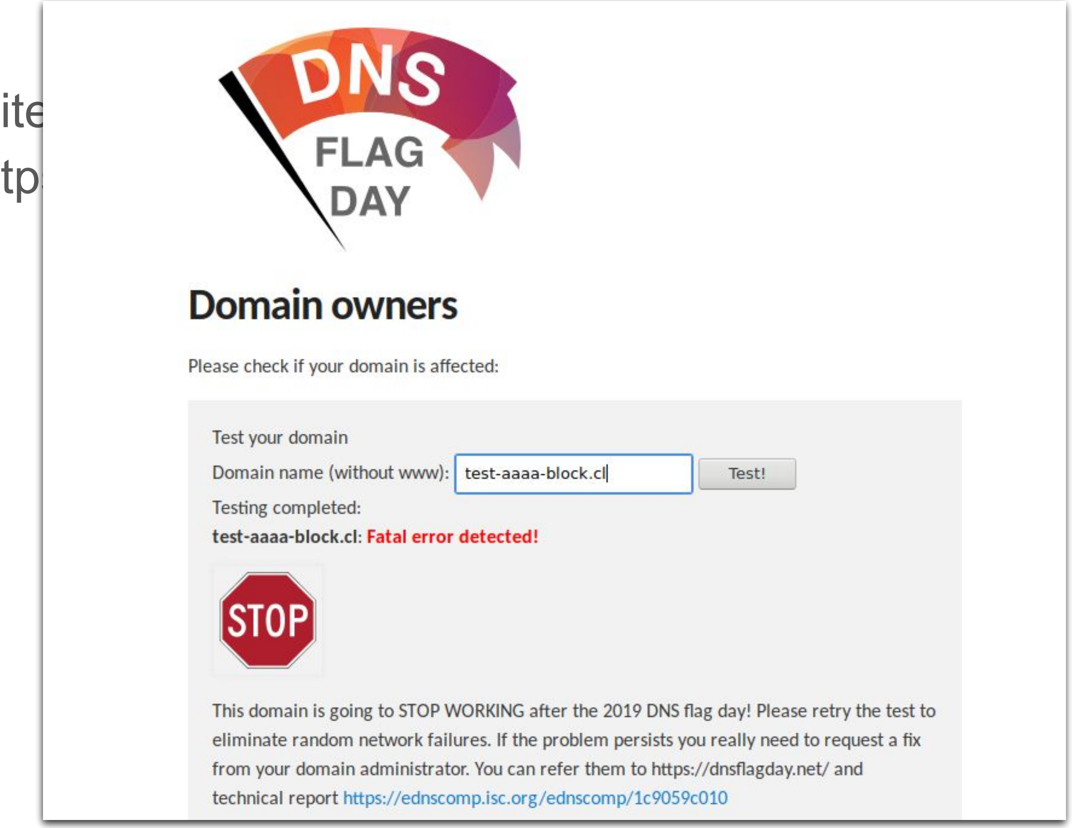
- Our measurements are consistent in about 1% of domain names affected
- For .com.br it’s ~24K domain names
- BUT, the good news: very easy to fix! ;)

How can I check my domain name?

- Web site, user-oriented:
  - https://dnsflagday.net/

How can I check my domain name?

- Web site
  - http



Domain owners

Please check if your domain is affected:

Test your domain

Domain name (without www): test-aaaa-block.cl

Testing completed:

test-aaaa-block.cl: Fatal error detected!

This domain is going to STOP WORKING after the 2019 DNS flag day! Please retry the test to eliminate random network failures. If the problem persists you really need to request a fix from your domain administrator. You can refer them to https://dnsflagday.net/ and technical report https://ednscomp.isc.org/ednscomp/1c9059c010

From https://dnsflagday.net (redacted)

How can I check my domain name?

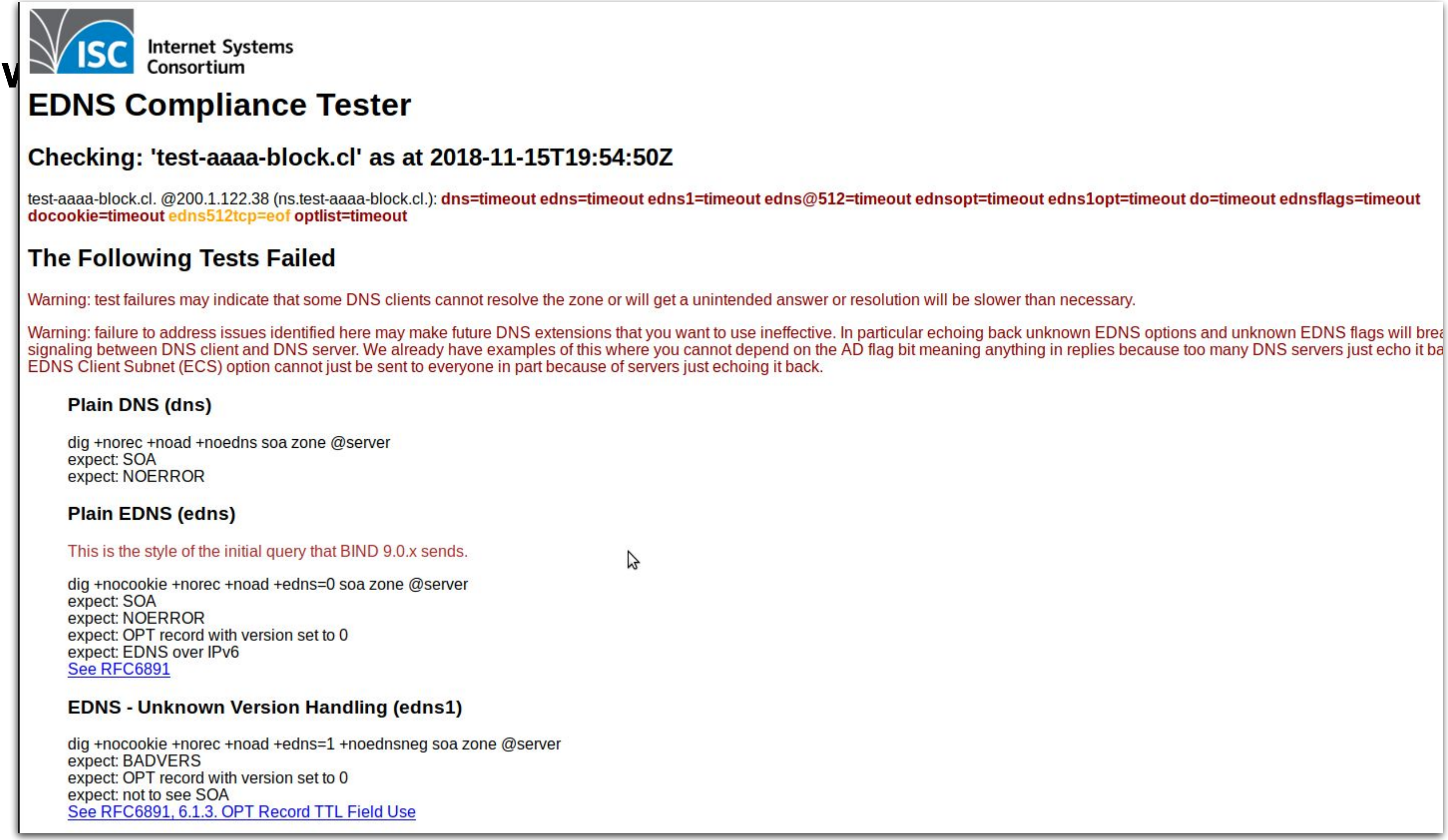
- Web site, user-oriented:
  - https://dnsflagday.net/

- ISC tool, expert-oriented:
  - https://ednscomp.isc.org/ednscomp

Hov

-

-



Internet Systems Consortium

EDNS Compliance Tester

Checking: 'test-aaaa-block.cl' as at 2018-11-15T19:54:50Z

test-aaaa-block.cl. @200.1.122.38 (ns.test-aaaa-block.cl.): **dns=timeout edns=timeout edns1=timeout edns@512=timeout ednsopt=timeout edns1opt=timeout do=timeout ednsflags=timeout docookie=timeout edns512tcp=eof optlist=timeout**

The Following Tests Failed

Warning: test failures may indicate that some DNS clients cannot resolve the zone or will get a unintended answer or resolution will be slower than necessary.

Warning: failure to address issues identified here may make future DNS extensions that you want to use ineffective. In particular echoing back unknown EDNS options and unknown EDNS flags will brea signaling between DNS client and DNS server. We already have examples of this where you cannot depend on the AD flag bit meaning anything in replies because too many DNS servers just echo it ba EDNS Client Subnet (ECS) option cannot just be sent to everyone in part because of servers just echoing it back.

Plain DNS (dns)

```
dig +norec +noad +noedns soa zone @server
expect: SOA
expect: NOERROR
```

Plain EDNS (edns)

This is the style of the initial query that BIND 9.0.x sends.

```
dig +nocookie +norec +noad +edns=0 soa zone @server
expect: SOA
expect: NOERROR
expect: OPT record with version set to 0
expect: EDNS over IPv6
```

See RFC6891

EDNS - Unknown Version Handling (edns1)

```
dig +nocookie +norec +noad +edns=1 +noednsneg soa zone @server
expect: BADVERS
expect: OPT record with version set to 0
expect: not to see SOA
```

See RFC6891, 6.1.3. OPT Record TTL Field Use

From https://ednscomp.isc.org/ednscomp

How can I correct the errors?

- Use a **modern** implementation of DNS software
- Use software that follows the **standards**
- Fix your **firewall** rules, especially around DPI of DNS traffic
- Re-test

Future work

- We plan to continue the collection monthly to identify trends
- Communication campaign to reduce the number of errors.
- We encourage other namespace operators (ccTLDs) to check their domains
- Watch the world burn on February 1st 2019

Questions

https://dnsflagday.net

Hugo Salgado, hsalgado@nic.cl

nic chile
SOMOS EL PUNTO CL

InternetNZ